

On the class of languages recognizable by 1-way quantum finite automata

Andris Ambainis¹, Arnolds Ķikusts², Māris Valdatš²

¹ Computer Science Division, University of California, Berkeley, CA94720, USA, ambainis@cs.berkeley.edu ***

² Institute of Mathematics and Computer Science, University of Latvia, Raiņa bulv. 29, Rīga, Latvia[†]
sd70053@lanet.lv, sd70066@lanet.lv

Abstract. It is an open problem to characterize the class of languages recognized by quantum finite automata (QFA). We examine some necessary and some sufficient conditions for a (regular) language to be recognizable by a QFA. For a subclass of regular languages we get a condition which is necessary and sufficient.

Also, we prove that the class of languages recognizable by a QFA is not closed under union or any other binary Boolean operation where both arguments are significant.

1 Introduction

A quantum finite automaton (QFA) is a theoretical model for a quantum computer with a finite memory.

If we compare them with their classical (non-quantum) counterparts, QFAs have both strengths and weaknesses. The strength of QFAs is shown by the fact that quantum automata can be exponentially more space efficient than deterministic or probabilistic automata [AF 98]. The weakness of QFAs is caused by the fact that any quantum process has to be reversible (unitary). This makes quantum automata unable to recognize some regular languages.

The first result of this type was obtained by Kondacs and Watrous [KW 97] who showed that there is a language that can be recognized by a deterministic finite automaton (DFA) but cannot be recognized by QFA. Later, Brodsky and Pippenger [BP 99] generalized the construction of [KW 97] and showed that any regular language that does not satisfy the partial order condition cannot be recognized by a QFA. They also conjectured that all regular languages satisfying the partial order condition can be recognized by a QFA.

In this paper, we disprove their conjecture. We show that, for a language to be recognizable by a 1-way QFA, its minimal deterministic automaton must not contain several “forbidden fragments”. One of these fragments is equivalent to the automaton not satisfying the partial order condition. The other fragments are new.

A somewhat surprising feature of our “forbidden fragments” is that they consist of several parts (corresponding to different beginnings of the word) and the language corresponding to every one of them can be recognized but one cannot simultaneously recognize the whole language without violating unitarity.

Our result implies that the set of languages recognizable by QFAs is not closed under union. In particular, if we consider the language consisting of all words in the alphabet $\{a, b\}$ that have an even number of a 's after the first b , this language is not recognizable by a QFA, although it is a union of two recognizable languages. (The first language consists of all words with an even number of a 's before the first b and an even number of a 's after the first b , the second language consists of all words with an odd number of a 's before the first b and an even number of a 's after it.) This answers a question of Brodsky and Pippenger [BP 99].

For a subclass of regular languages (languages that do not contain “two cycles in a row” construction shown in Fig. 3), we show that our conditions are necessary and sufficient for a language to be recognizable

*** Research supported by Berkeley Fellowship for Graduate Studies and, in part, NSF Grant CCR-9800024.

[†] Research supported by Grant No.96.0282 from the Latvian Council of Science and European Commission, contract IST-1999-11234.

by a QFA. For arbitrary regular languages, we only know that these conditions are necessary but we do not know if all languages satisfying them can be recognized by a QFA.

1.1 Definitions

Quantum finite automata (QFA) were introduced independently by Moore and Crutchfield [MC 97] and Kondacs and Watrous [KW 97]. In this paper, we consider the more general definition of QFAs [KW 97] (which includes the definition of [MC 97] as a special case).

Definition 1.1. A QFA is a tuple $M = (Q; \Sigma; V; q_0; Q_{acc}; Q_{rej})$ where Q is a finite set of states, Σ is an input alphabet, V is a transition function, $q_0 \in Q$ is a starting state, and $Q_{acc} \subseteq Q$ and $Q_{rej} \subseteq Q$ are sets of accepting and rejecting states ($Q_{acc} \cap Q_{rej} = \emptyset$). The states in Q_{acc} and Q_{rej} , are called halting states and the states in $Q_{non} = Q - (Q_{acc} \cup Q_{rej})$ are called non halting states. κ and $\$$ are symbols that do not belong to Σ . We use κ and $\$$ as the left and the right endmarker, respectively. The working alphabet of M is $\Gamma = \Sigma \cup \{\kappa; \$\}$.

The state of M can be any superposition of states in Q (i. e., any linear combination of them with complex coefficients). We use $|q\rangle$ to denote the superposition consisting of state q only. $l_2(Q)$ denotes the linear space consisting of all superpositions, with l_2 -distance on this linear space.

The transition function V is a mapping from $\Gamma \times l_2(Q)$ to $l_2(Q)$ such that, for every $a \in \Gamma$, the function $V_a : l_2(Q) \rightarrow l_2(Q)$ defined by $V_a(x) = V(a, x)$ is a unitary transformation (a linear transformation on $l_2(Q)$ that preserves l_2 norm).

The computation of a QFA starts in the superposition $|q_0\rangle$. Then transformations corresponding to the left endmarker κ , the letters of the input word x and the right endmarker $\$$ are applied. The transformation corresponding to $a \in \Gamma$ consists of two steps.

1. First, V_a is applied. The new superposition ψ' is $V_a(\psi)$ where ψ is the superposition before this step.
2. Then, ψ' is observed with respect to $E_{acc}, E_{rej}, E_{non}$ where $E_{acc} = \text{span}\{|q\rangle : q \in Q_{acc}\}$, $E_{rej} = \text{span}\{|q\rangle : q \in Q_{rej}\}$, $E_{non} = \text{span}\{|q\rangle : q \in Q_{non}\}$. It means that if the system's state before the measurement was

$$\psi' = \sum_{q_i \in Q_{acc}} \alpha_i |q_i\rangle + \sum_{q_j \in Q_{rej}} \beta_j |q_j\rangle + \sum_{q_k \in Q_{non}} \gamma_k |q_k\rangle$$

then the measurement accepts ψ' with probability $\Sigma \alpha_i^2$, rejects with probability $\Sigma \beta_j^2$ and continues the computation (applies transformations corresponding to next letters) with probability $\Sigma \gamma_k^2$ with the system having state $\psi = \Sigma \gamma_k |q_k\rangle$.

We regard these two transformations as reading a letter a . We use V'_a to denote the transformation consisting of V_a followed by projection to E_{non} . This is the transformation mapping ψ to the non-halting part of $V_a(\psi)$. We use V'_w to denote the product of transformations $V'_w = V'_{a_n} V'_{a_{n-1}} \dots V'_{a_2} V'_{a_1}$, where a_i is the i -th letter of the word w . We also use ψ_y to denote the non-halting part of QFA's state after reading the left endmarker κ and the word $y \in \Sigma^*$. From the notation it follows that $\psi_w = V'_{\kappa w}(|q_0\rangle)$.

We will say that an automaton recognizes a language L with probability p ($p > \frac{1}{2}$) if it accepts any word $x \in L$ with probability $\geq p$ and rejects any word $x \notin L$ with probability $\geq p$.

1.2 Previous work

The previous work on 1-way quantum finite automata (QFAs) has mainly considered 3 questions:

1. What is the class of languages recognized by QFAs?
2. What accepting probabilities can be achieved?
3. How does the size of QFAs (the number of states) compare to the size of deterministic (probabilistic) automata?

In this paper, we consider the first question. The first results in this direction were obtained by Kondacs and Watrous [KW 97].

Theorem 1.1. [KW 97]

1. All languages recognized by 1-way QFAs are regular.
2. There is a regular language that cannot be recognized by a 1-way QFA with probability $\frac{1}{2} + \epsilon$ for any $\epsilon > 0$.

Brodsky and Pippenger [BP 99] generalized the second part of Theorem 1.1 by showing that any language satisfying a certain property is not recognizable by a QFA.

Theorem 1.2. [BP 99] Let L be a language and M be its minimal automaton (the smallest DFA recognizing L). Assume that there is a word x such that M contains states q_1, q_2 satisfying:

1. $q_1 \neq q_2$,
2. If M starts in the state q_1 and reads x , it passes to q_2 ,
3. If M starts in the state q_2 and reads x , it passes to q_2 , and
4. There is a word y such that if M starts in q_2 and reads y , it passes to q_1 ,

then L cannot be recognized by any 1-way quantum finite automaton (Fig.1).

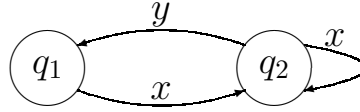


Fig. 1. Conditions of theorem 1.2

A language L with the minimal automaton not containing a fragment of Theorem 1.2 is called *satisfying the partial order condition* [MT 69]. [BP 99] conjectured that any language satisfying the partial order condition is recognizable by a 1-way QFA. In this paper, we disprove this conjecture.

Another direction of research is studying the accepting probabilities of QFAs. This direction started with Ambainis and Freivalds [AF 98] showing that the language a^*b^* is recognizable by a QFA with probability 0.68... but not with probability $7/9 + \epsilon$ for any $\epsilon > 0$. This showed that the classes of languages recognizable with different probabilities are different. Next results in this direction were obtained by [ABFK 99] who studied the probabilities with which the languages $a_1^* \dots a_n^*$ can be recognized.

There is also a lot of results about the number of states needed for QFA to recognize different languages. In some cases, it can be exponentially less than for deterministic or even for probabilistic automata [AF 98, K 98]. In other cases, it can be exponentially bigger than for deterministic automata [ANTV 98, N 99].

A good survey about quantum automata is Gruska [G 00].

2 Main results

2.1 Necessary condition

First, we give the new condition which implies that the language is not recognizable by a QFA. Similarly to the previous condition (Theorems 1.2), it can be formulated as a condition about the minimal deterministic automaton of a language.

Theorem 2.1. *Let L be a language. Assume that there are words x, y, z_1, z_2 such that its minimal automaton M contains states q_1, q_2, q_3 satisfying:*

1. $q_2 \neq q_3$,
2. if M starts in the state q_1 and reads x , it passes to q_2 ,
3. if M starts in the state q_2 and reads x , it passes to q_2 ,
4. if M starts in the state q_1 and reads y , it passes to q_3 ,
5. if M starts in the state q_3 and reads y , it passes to q_3 ,
6. for all words $t \in (x|y)^*$ there exists a word $t_1 \in (x|y)^*$ such that if M starts in the state q_2 and reads tt_1 , it passes to q_2 ,
7. for all words $t \in (x|y)^*$ there exists a word $t_1 \in (x|y)^*$ such that if M starts in the state q_3 and reads tt_1 , it passes to q_3 ,
8. if M starts in the state q_2 and reads z_1 , it passes to an accepting state,
9. if M starts in the state q_2 and reads z_2 , it passes to a rejecting state,
10. if M starts in the state q_3 and reads z_1 , it passes to a rejecting state,
11. if M starts in the state q_3 and reads z_2 , it passes to an accepting state.

Then L cannot be recognized by a 1-way QFA.

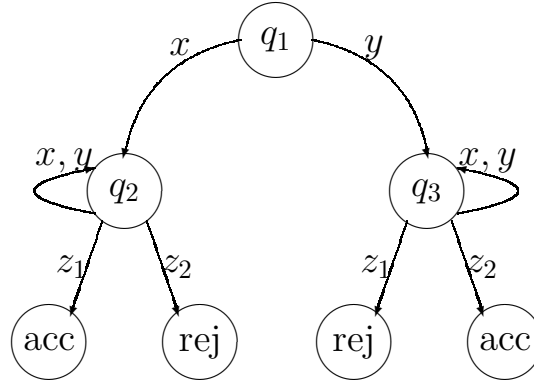


Fig. 2. Conditions of theorem 2.1, conditions 6 and 7 are shown symbolically

Proof. We use a lemma from [BV 97].

Lemma 2.1. *If ψ and ϕ are two quantum states and $\|\psi - \phi\| < \varepsilon$ then the total variational distance between the probability distributions generated by the same measurement on ψ and ϕ is at most¹ 2ε .*

We also use a lemma from [AF 98].

Lemma 2.2. *Let $x \in \Sigma^+$. There are subspaces E_1, E_2 such that $E_{non} = E_1 \oplus E_2$ and*

- (i) *If $\psi \in E_1$, then $V'_x(\psi) \in E_1$ and $\|V'_x(\psi)\| = \|\psi\|$,*
- (ii) *If $\psi \in E_2$, then $\|V'_{x^k}(\psi)\| \rightarrow 0$ when $k \rightarrow \infty$.*

¹ The lemma in [BV 97] has 4ε but it can be improved to 2ε .

Lemma 2.2 can be viewed as a quantum counterpart of the *classification of states for Markov chains* [KS 76]. The classification of states divides the states of a Markov chain into *ergodic* sets and *transient* sets. If the Markov chain is in an ergodic set, it never leaves it. If it is in a transient set, it leaves it with probability $1 - \epsilon$ for an arbitrary $\epsilon > 0$ after sufficiently many steps.

In the quantum case, E_1 is the counterpart of an ergodic set: if the quantum random process defined by repeated reading of x is in a state $\psi \in E_1$, it stays in E_1 . E_2 is a counterpart of a transient set: if the state is $\psi \in E_2$, E_2 is left (for an accepting or rejecting state) with probability arbitrarily close to 1 after sufficiently many x 's.

The next Lemma is our generalization of Lemma 2.2 for the case of two different words x and y .

Lemma 2.3. *Let $x, y \in \Sigma^+$. There are subspaces E_1, E_2 such that $E_{non} = E_1 \oplus E_2$ and*

- (i) *If $\psi \in E_1$, then $V'_x(\psi) \in E_1$ and $V'_y(\psi) \in E_1$ and $\|V'_x(\psi)\| = \|\psi\|$ and $\|V'_y(\psi)\| = \|\psi\|$,*
- (ii) *If $\psi \in E_2$, then for any $\epsilon > 0$, there exists a word $t \in (x|y)^*$ such that $\|V'_t(\psi)\| < \epsilon$.*

Proof. We use E_1^z to denote the space E_1 from Lemma 2.2 for a word z . We define $E_1 = \bigcap_{z \in (x|y)^*} E_1^z$. E_2 consists of all vectors in E_{non} orthogonal to E_1 . Next, we check that both (i) and (ii) are true.

- (i) It is easy to see that, for all $t \in (x|y)^*$, $\|V'_t(\psi)\| = \|\psi\|$ due to $\psi \in E_1^t$.

We also need to prove that $V'_x(\psi) \in E_1$ and $V'_y(\psi) \in E_1$. For a contradiction, assume there are $\psi \in E_1$ and $t_1 \in (x|y)^*$ such that $V'_{t_1}(\psi) \notin E_1$. Then, by definition of E_1 , there also exists $t_2 \in (x|y)^*$ such that $V'_{t_1}(\psi)$ does not belong to $E_1^{t_2}$. Lemma 2.2 implies that the norm of $V'_{t_1}(\psi)$ can be decreased by repeated applications of V'_{t_2} . A contradiction with $\|V'_t(\psi)\| = \|\psi\|$ for all t .

- (ii) Clearly, if ψ belongs to E_2 then for all $t \in (x|y)^*$ the superposition $V'_t(\psi)$ also belongs to E_2 because V_x and V_y are unitary and map E_1 to itself (and, therefore, any vector orthogonal to E_1 is mapped to a vector orthogonal to E_1).

$\|V'_t(\psi)\|$ does not increase if we extend the word t to the right and it is bounded from below by 0. Hence, for any fixed ϵ we can find a $t \in (x|y)^*$ such that

$$\|V'_t(\psi)\| - \|V'_{tw}(\psi)\| < \epsilon$$

for all $w \in (x|y)^*$. We define a sequence of such words t_1, t_2, t_3, \dots for $\epsilon, \frac{\epsilon}{2}, \frac{\epsilon}{4}, \dots$. $V'_{t_1}(\psi), V'_{t_2}(\psi), V'_{t_3}(\psi), \dots$ is a bounded sequence in a finite dimensional space. Therefore, it has a limit point ψ' . We will show that $\psi' = 0$.

First, notice that $\psi' \in E_2$ because it is a limit of a subsequence of $V'_{t_1}(\psi), V'_{t_2}(\psi), V'_{t_3}(\psi), \dots$ and all $V'_{t_i}(\psi)$ belong to E_2 . Therefore, if $\psi' \neq 0$ then ψ' has nonzero E_2^z component for some $z \in (x|y)^*$. Reading sufficiently many z would decrease this component, decreasing the norm of ψ' .

This contradicts the fact that, for any w , $\|\psi'\| = \|V'_w(\psi')\|$ (since $\|\psi'\| - \|V'_w(\psi')\|$ is less than any $\epsilon > 0$ which is true because ψ' is the limit of $V'_{t_1}(\psi), V'_{t_2}(\psi), V'_{t_3}(\psi), \dots$).

Therefore, $\psi' = 0$. This completes the proof of lemma. \square

Let L be a language such that its minimal automaton M contains the "forbidden construction" and M_q be a QFA. We show that M_q does not recognize L .

Let w be a word after reading which M is in the state q_1 . Let $\psi_w = \psi_w^1 + \psi_w^2$, $\psi_w^1 \in E_1$, $\psi_w^2 \in E_2$. We find a word $a \in (x|y)^*$ such that after reading xa M is in the state q_2 and the norm of $\psi_{wxa}^2 = V'_a(\psi_w^2)$ is at most some fixed $\epsilon > 0$. (Such word exists due to Lemma 2.3 and conditions 6 and 7.) We also find a word b such that $\|\psi_{wyb}^2\| \leq \epsilon$.

Because of unitarity of V'_x and V'_y on E_1 (part (i) of Lemma 2.3), there exist integers i and j such that $\|\psi_{w(xa)^i}^1 - \psi_w^1\| \leq \epsilon$ and $\|\psi_{w(yb)^j}^1 - \psi_w^1\| \leq \epsilon$.

Let p be the probability of M_q accepting while reading κw . Let p_1 be the probability of accepting while reading $(xa)^i$ with a starting state ψ_w , p_2 be the probability of accepting while reading $(yb)^j$ with a starting state ψ_w and p_3, p_4 be the probabilities of accepting while reading $z_1\$$ and $z_2\$$ with a starting state ψ_w^1 .

Let us consider four words $\kappa w(xa)^i z_1 \$$, $\kappa w(xa)^i z_2 \$$, $\kappa w(yb)^j z_1 \$$, $\kappa w(yb)^j z_2 \$$.

Lemma 2.4. M_q accepts $\kappa w(xa)^i z_1 \$$ with probability at least $p + p_1 + p_3 - 4\epsilon$ and at most $p + p_1 + p_3 + 4\epsilon$.

Proof. The probability of accepting while reading κw is p . After that, M_q is in the state ψ_w and reading $(xa)^i$ in this state causes it to accept with probability p_1 .

The remaining state is $\psi_{w(xa)^i} = \psi_{w(xa)^i}^1 + \psi_{w(xa)^i}^2$. If it was ψ_w^1 , the probability of accepting while reading the rest of the word $(z_1 \$)$ would be exactly p_3 . It is not quite ψ_w^1 but it is close to ψ_w^1 . Namely, we have

$$\|\psi_{w(xa)^i} - \psi_w^1\| \leq \|\psi_{w(xa)^i}^2\| + \|\psi_{w(xa)^i}^1 - \psi_w^1\| \leq \epsilon + \epsilon = 2\epsilon.$$

By Lemma 2.1, this means that the probability of accepting during $z_1 \$$ is between $p_3 - 4\epsilon$ and $p_3 + 4\epsilon$. \square

Similarly, on the second word M_q accepts with probability between $p + p_1 + p_4 - 4\epsilon$ and $p + p_1 + p_4 + 4\epsilon$. On the third word M_q accepts with probability between $p + p_2 + p_3 - 4\epsilon$ and $p + p_2 + p_3 + 4\epsilon$. On the fourth word M_q accepts with probability $p + p_2 + p_4 - 4\epsilon$ and $p + p_2 + p_4 + 4\epsilon$.

This means that the sum of accepting probabilities of two words that belong to L (the first and the fourth words) differs from the sum of accepting probabilities of two words that do not belong to L (the second and the third) by at most 16ϵ . Hence, the probability of correct answer of M_q on one of these words is at most $\frac{1}{2} + 4\epsilon$. Since such 4 words can be constructed for arbitrarily small ϵ , this means that M_q does not recognize L . \square

2.2 Necessary and sufficient condition

For languages whose minimal automaton does not contain the construction of Figure 3, this condition (together with Theorem 1.2) is necessary and sufficient.

Theorem 2.2. Let U be the class of languages whose minimal automaton does not contain "two cycles in a row" (Fig. 3). A language that belongs to U can be recognized by a 1-way QFA if and only if its minimal deterministic automaton does not contain the "forbidden construction" from Theorem 1.2 and the "forbidden construction" from Theorem 2.1.

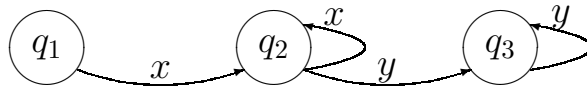


Fig. 3. Conditions of theorem 2.2

Proof. Let M be the minimal deterministic automaton of a language L . If it contains at least one of "forbidden constructions" of Theorems 1.2 and 2.1, then L cannot be recognized by a 1-way QFA. We now show that, if M does not contain any of the two "forbidden constructions" and does not contain "two cycles in a row" construction then L can be recognized by a QFA.

Let q_0 be the starting state of M and V be the transition function of the automaton M . $V(q, x)$ denotes the state to which M goes if it reads the word x in the state q .

We will construct a QFA for L by splitting M into pieces A, B_1, \dots, B_n , constructing a reversible finite automaton for each of those pieces and then combining these reversible automata.

Let B be the set of all states q such that after reading any word in q , there exists a word such that M passes back to the state q . We split B into connected components B_1, B_2, \dots, B_n . Two different states q_i and q_j belong to the same B_k iff q_i is reachable from q_j and q_j is reachable from q_i . Let A be the set of all remaining states, i. e., the states that do not belong to $B = B_1 \cup B_2 \cup \dots \cup B_n$.

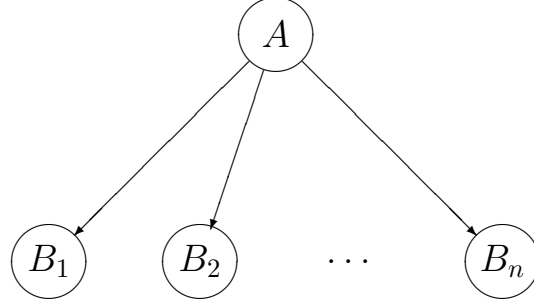


Fig. 4. Division of M

Lemma 2.5. *For every letter a and every state q of B_i , there is exactly one $q' \in B_i$ such that reading a in q' leads to q , i. e., every letter induces a permutation of states in B_i .*

Proof. Let q be a state in B_i and $a \in \Sigma$. For a contradiction, assume that there are two states $q' \in B_i$ and $q'' \in B_i$ such that $V(q', a) = V(q'', a) = q$.

Then, there exist words x' and x'' such that $V(q, x') = q''$ and $V(q'', x') = q'$. (This is true because every state in B_i is reachable from every other state in B_i .)

However, this means that B_i contains the “forbidden construction” of Theorem 1.2, with $q_1 = q'$, $q_2 = q''$, $x = ax''$ and $y = x'$. A contradiction. \square

Such automata B_i are called *permutation automata*.

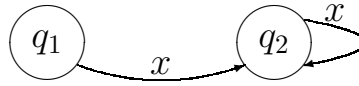


Fig. 5. Conditions of Lemma 2.6

Lemma 2.6. *A does not contain a fragment of the form shown in Fig. 5 with q_1 and q_2 being two different states of A and $x \in \Sigma^+$.*

Proof. For a contradiction, assume that A contains such a fragment.

By definition of A and B , $q_2 \in A$ implies that there is a word z such that reading z in q_2 leads to a state q'_2 and q_2 is not reachable from q'_2 .

Consider the states $V(q_2, z), V(q_2, z^2), \dots$. M has a finite number of states. Therefore, there must be j and k such that $V(q_2, z^j) = V(q_2, z^{j+k})$. Notice that this implies $V(q_2, z^{j'}) = V(q_2, z^{j'+k})$ for all $j' \geq j$.

Let i be the smallest number such that $i \geq j$ and i is divisible by k . Define $q_3 = V(q_2, z^i)$. Then, $V(q_2, z^i) = V(q_2, z^{i+k}) = V(q_2, z^{i+2k}) = \dots = V(q_2, z^{2i})$ (because i is divisible by k), i. e., $q_3 = V(q_3, z^i)$.

We have shown that q_1, q_2, q_3 form a “two cycles in a row” construction with $y = z^i$. A contradiction. \square

By a theorem from [AF 98], any language recognizable by a deterministic automaton which does not contain the construction of Fig. 5 is recognizable by a reversible finite automaton (RFA). (A reversible finite automaton is a deterministic automaton in which, for every state q and letter a , there is at most one state q' such that reading a in q' leads to q .)

Any reversible automaton is a special case of a quantum automaton. (If, for every state q and every letter a , there is one q' such that reading a leads to q , the letter a induces a permutation on states of automaton and the corresponding transformation of a quantum automaton is clearly unitary.)

Therefore, the language recognized by A is recognized by a QFA as well. Also, permutation automata B_1, \dots, B_n are special cases of reversible automata. Therefore, they can be replaced by equivalent QFAs. We will construct a QFA for L by combining those QFAs.

However, before that, we must solve one problem. Even if the state of M after reading a word x is in B_i , the starting state of M can be in A . If we want to use the permutation automaton for B_i to recognize a part of L , we must define one of states in B_i as the starting state. The next two lemmas show that this is possible.

Lemma 2.7. *If the minimal automaton M contains the construction of Fig. 6, the states q_2 and q_3 cannot be in the same B_i .*

Proof. Let us suppose the opposite.

q_2 and q_3 are different states of the minimal deterministic automaton. Therefore, there exists a word a such that $V(q_2, a)$ is an accepting state (or a rejecting state) and $V(q_3, a)$ is a rejecting state (or an accepting state).

Also, there is no word l such that $V(q_2, l)$ is a rejecting state (or an accepting state) and $V(q_3, l)$ is an accepting state (or a rejecting state) because, otherwise, M would contain the construction of Theorem 2.1.

We denote $V(q_2, a)$ by q_{acc} and $V(q_3, a)$ by q_{rej} . There exists a word b such that $V(q_{rej}, b) = q_{acc}$ (because all states in B_i can be reached from one another). Moreover, the states $V(q_2, ab)$ and $V(q_3, ab)$ are accepting states ($V(q_3, ab)$ is accepting because $V(q_3, ab) = V(q_{rej}, b) = q_{acc}$ and $V(q_2, ab)$ is accepting because, if it was rejecting, q_1, q_2 and q_3 would form the construction of Theorem 2.1 with a and ab as z_1 and z_2). Similarly, the states $V(q_2, abb)$ and $V(q_3, abb)$ are accepting states, the states $V(q_2, abbb)$ and $V(q_3, abbb)$ are accepting states and so on. However, there exists k such that $V(q_3, ab^k) = V(q_3, a) = q_{rej}$ (because B_i is a permutation automaton and, therefore, it must return to the starting state after some number of b 's). This gives us the contradiction. \square

Lemma 2.8. *For each part B_i , there is a state q such that if $V(q_0, x)$ belongs to B_i then $V(q_0, x) = V(q, x)$.*

Proof. Let $V(q_0, x) \in B_i$. Then, there is a unique $q \in B_i$ such that $V(q_0, x) = V(q, x)$. (This is true because B_i is a permutation automaton and every state has a unique preceding state.) We must show that this state q does not depend on the word x .

Assume this is not true. Then, there are words x and y such that $V(q_0, x) = V(q_2, x)$ and $V(q_0, y) = V(q_3, y)$ and $q_2 \neq q_3$ (and $V(q_2, x), q_2, V(q_3, y), q_3$ are all in B_i).

Let $q_4 = V(q_2, x)$ and $q_5 = V(q_3, y)$. Then, there exist $j \in \mathbb{N}$ and $k \in \mathbb{N}$ such that $V(q_4, x^j) = q_4$ and $V(q_5, y^k) = q_5$. (Again, we are using the fact that B_i is a permutation automaton, and, therefore, if it reads the same word many times, it returns to the same state at some point.)

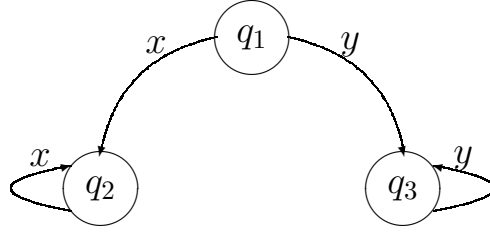


Fig. 6.

This implies $V(q_4, x^{j-1}) = q_2$ and $V(q_5, y^{k-1}) = q_3$ (because $V(q_2, x) = q_4$ and $V(q_3, y) = q_5$ and, in a permutation automaton, q such that $V(q, x) = q_4$ must be unique). Therefore, $V(q_0, x^j) = V(q_4, x^{j-1}) = q_2$ and $V(q_2, x^j) = V(q_4, x^{j-1}) = q_2$. Similarly, $V(q_0, y^k) = V(q_3, y^k) = q_3$.

This means that B_i contains the states q_2 and q_3 from the construction shown in Figure 6 (with x^j and y^k instead of x and y and q_0 instead of q_1). By Lemma 2.7, this is impossible. A contradiction. \square

We denote these states as q_i . Let B'_i be the automaton B_i with q_i as the starting state. Let L_i be the language recognized by B'_i .

Lemma 2.9. *For any $i, j \in \{1, \dots, n\}$, either $L_i \subseteq L_j$ or $L_j \subseteq L_i$.*

Proof. Let x and y be such that $V(q_0, x) = q_i$ and $V(q_0, y) = q_j$. (x and y exist because, otherwise, q_i or q_j would be unreachable from the starting state q_0 .) By Lemma 2.8, $V(q_i, x) = q_i$ and $V(q_j, y) = q_j$.

For a contradiction, assume that neither $L_i \subseteq L_j$ nor $L_j \subseteq L_i$ is true. Then, there are words $z_1 \in L_i - L_j$ and $z_2 \in L_j - L_i$ and we get the “forbidden construction” of Theorem 2.1. \square

Let a_i denote the number of $j \in \{1, \dots, n\}$ such that $L_j \subseteq L_i$. A' denotes the corresponding reversible automaton for the automaton A with one modification: when the automaton M passes to a state of $B_1 \cup B_2 \cup \dots \cup B_n$ A' accepts with probability $\frac{n-a_i}{n+1}$ and rejects with probability $\frac{a_i+1}{n+1}$.

Next, we define a QFA recognizing the language L : it works as A' with probability $p = \frac{n+1}{2n+1}$ (with amplitude $\sqrt{\frac{n+1}{2n+1}}$) and as B_i with probability $\frac{1}{2n+1}$ (with amplitude $\frac{1}{\sqrt{2n+1}}$) for each i .

Case 1. $V(q_0, x) \in A$. The QFA recognizes x with probability p .

Case 2. $V(q_0, x) \in B_i$ and $x \in L$. The automaton A' accepts with probability $\frac{n-a_i}{n+1}$. Moreover, x is accepted by at least a_i automata from B'_1, B'_2, \dots, B'_n . This means that the total probability of accepting is at least

$$\frac{n-a_i}{n+1} \cdot \frac{n+1}{2n+1} + \frac{a_i+1}{2n+1} = \frac{n+1}{2n+1} = p.$$

Case 3. $V(q_0, x) \in B_i$ and $x \notin L$. Similarly to the previous case, the total probability of rejecting is at least p . \square

3 Non-closure under union

3.1 Non-closure result

In particular, Theorem 2.1 implies that the class of languages recognized by QFAs is not closed under union.

Let L_1 be the language consisting of all words that start with any number of letters a and after first letter b (if there is one) there is an odd number of letters a . Its minimal automaton G_1 is shown in Fig.7.

This language satisfies the conditions of Theorem 2.1. (q_1, q_2 and q_3 of Theorem 2.1 are just q_1, q_2 and q_3 of G_1 . x, y, z_1 and z_2 are b, aba, ab and b .) Hence, it cannot be recognized by a QFA.

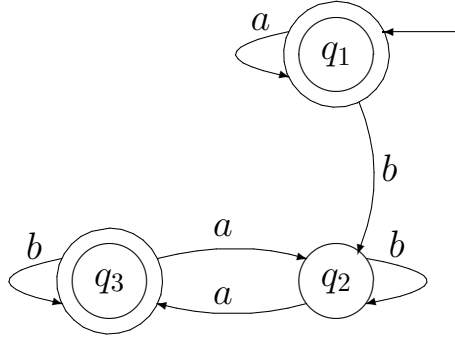


Fig. 7. Automaton G_1

Consider 2 other languages L_2 and L_3 defined as follows.

L_2 consists of all words which start with an even number of letters a and after first letter b (if there is one) there is an odd number of letters a .

L_3 consists of all words which start with an odd number of letters a and after first letter b (if there is one) there is an odd number of letters a .

It is easy to see that $L_1 = L_2 \cup L_3$.

The minimal automata G_2 and G_3 are shown in Fig.8 and Fig.9. They do not contain any of the “forbidden constructions” of Theorem 2.2. Therefore, L_2 and L_3 can be recognized by a QFA and we get

Theorem 3.1. *There are two languages L_2 and L_3 which are recognizable by a QFA but the union of them $L_1 = L_2 \cup L_3$ is not recognizable by a QFA.*

Corollary 3.1. *The class of languages recognizable by a QFA is not closed under union.*

This answers a question of Brodsky and Pippenger [BP 99].

As $L_2 \cap L_3 = \emptyset$ then also $L_1 = L_2 \Delta L_3$. So the class of languages recognizable by QFA is not closed under symmetric difference. From this and from the fact that this class is closed under complement, it easily follows:

Corollary 3.2. *The class of languages recognizable by a QFA is not closed under any binary boolean operation where both arguments are significant.*

3.2 Another construction of QFAs

Instead of using the general construction of Theorem 2.2, we can also use a construction specific to languages L_2 and L_3 . This gives simpler QFAs and achieves a better probability of correct answer. (Theorem 2.2 gives QFAs for L_2 and L_3 with the probability of correct answer $3/5$. Our construction below achieves the probability of correct answer $2/3$.)

We construct two quantum automata K_2 and K_3 which recognize languages L_2 and L_3 . Like G_2 and G_3 they differ only in a starting state.

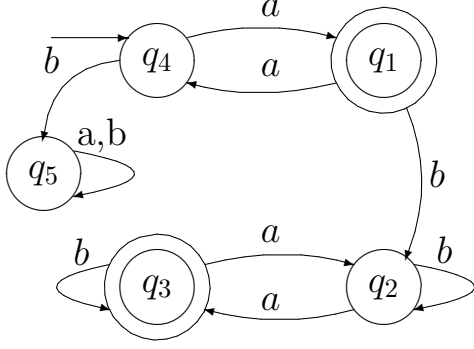


Fig. 8. Automaton G_2

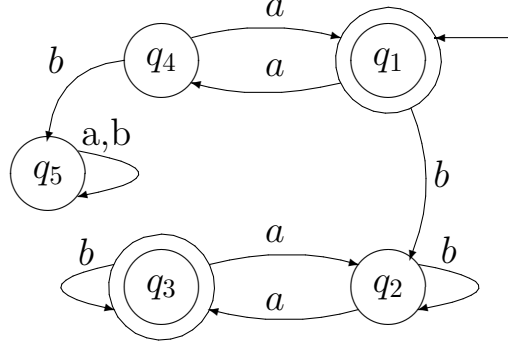


Fig. 9. Automaton G_3

The automaton K_2 consists of 8 states: $q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8$, where $Q_{non} = \{q_1, q_2, q_3, q_4\}$, $Q_{acc} = \{q_5, q_8\}$, $Q_{rej} = \{q_6, q_7\}$. The unitary transform matrices V_κ , V_a , V_b and V_\S are:

$$V_\kappa = \begin{pmatrix} \sqrt{\frac{2}{3}} & \sqrt{\frac{1}{3}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \sqrt{\frac{1}{3}} & -\sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -\sqrt{\frac{2}{3}} & \sqrt{\frac{1}{3}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\frac{2}{3}} & \sqrt{\frac{1}{3}} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, V_a = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$V_b = \begin{pmatrix} 0 & 0 & 0 & \sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \sqrt{\frac{1}{2}} & 0 & 0 & 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ \sqrt{\frac{1}{2}} & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, V_\S = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The starting state is q_1 for K_2 and q_4 for K_3 . Next, we show that K_2 works similarly to G_2 .

The state q_1 in G_2 corresponds to $\psi_1 = \sqrt{\frac{2}{3}}|q_1\rangle + \sqrt{\frac{1}{3}}|q_2\rangle$ in K_2 .

The state q_2 in G_2 corresponds to $\psi_2 = \sqrt{\frac{1}{3}}|q_2\rangle$ in K_2 .

The state q_3 in G_2 corresponds to $\psi_3 = \sqrt{\frac{1}{3}}|q_3\rangle$ in K_2 .

The state q_4 in G_2 corresponds to $\psi_4 = \sqrt{\frac{2}{3}}|q_4\rangle + \sqrt{\frac{1}{3}}|q_3\rangle$ in K_2 .

1. After reading the left endmarker κ K_2 is in the state $V'_\kappa(|q_1\rangle) = \psi_1$. G_2 is in its starting state q_1 .
2. If by reading the letter a the automaton G_2 passes from q_1 to q_4 or back then the state of K_2 changes from ψ_1 to ψ_4 or back.

3. If K_2 receives the letter b in the state ψ_4 then it rejects the input with probability $\frac{2}{3}$. This is correct because G_2 passes from q_4 to the "all rejecting" state q_5 .
4. If G_2 receives the letter b in the state q_1 it passes to q_3 . If K_2 receives the letter b in the state ψ_1 , it passes to the state $\frac{1}{\sqrt{3}}|q_2\rangle + \frac{1}{\sqrt{3}}|q_5\rangle + \frac{1}{\sqrt{3}}|q_6\rangle$ and after the measurement accepts the input with probability $\frac{1}{3}$, rejects the input with the same probability $\frac{1}{3}$, or continues in the state ψ_2 .
5. If by reading the letter a the automaton G_2 passes from q_2 to q_3 or back then the state of K_2 changes from ψ_2 to ψ_3 or back. By reading the letter b G_2 passes from q_2 to q_2 and from q_3 to q_3 . K_2 passes from ψ_2 to ψ_2 and from ψ_3 to ψ_3 .
6. If K_2 receives the right endmarker in state ψ_1 then the input is accepted with probability $\frac{2}{3}$.
7. If K_2 receives the right endmarker in state ψ_2 then the input is rejected with probability $\frac{1}{3}$ and as it was rejected with the same probability so far, the total probability to reject the input is $\frac{2}{3}$.
8. If K_2 receives the right endmarker in state ψ_3 then the input is accepted with probability $\frac{1}{3}$ and as it was accepted with the same probability so far the total probability to accept the input is $\frac{2}{3}$.
9. If K_2 receives the right endmarker in state ψ_4 then the input is rejected with probability $\frac{2}{3}$.

This shows that, whenever G_2 is in a state q_i ($i \in \{1, 2, 3, 4\}$), K_2 is in the corresponding state ψ_i . Also, this shows that K_2 accepts input with probability $\frac{2}{3}$ iff it receives right endmarker $\$$ in one of states ψ_1 or ψ_3 corresponding to q_1 and q_3 , the only accepting states in G_1 . So, we can conclude that K_2 accepts the language L_2 with probability $\frac{2}{3}$. Similarly, we can show that K_3 accepts L_3 with probability $\frac{2}{3}$.

Thus, we have shown

Theorem 3.2. *There are two languages L_2 and L_3 which are recognizable by a QFA with probability $\frac{2}{3}$ but the union of them $L_1 = L_2 \cup L_3$ is not recognizable with a QFA (with any probability $1/2 + \epsilon$, $\epsilon > 0$).*

3.3 On accepting probabilities

The probabilities for L_2 and L_3 achieved in Theorem 3.2 are the best possible, as shown by the following theorem.

Theorem 3.3. *If 2 languages L_1 and L_2 are recognizable by a QFA with probabilities p_1 and p_2 and $\frac{1}{p_1} + \frac{1}{p_2} < 3$ then $L = L_1 \cup L_2$ is also recognizable by QFA with probability $\frac{2p_1p_2}{p_1+p_2+p_1p_2}$.*

Proof. We have a QFA K_1 which accepts L_1 with probability p_1 and a QFA K_2 which accepts L_2 with probability p_2 . We will make a QFA K which will work like this:

1. Runs K_1 with probability $\frac{p_2}{p_1+p_2+p_1p_2}$,
2. Runs K_2 with probability $\frac{p_1}{p_1+p_2+p_1p_2}$,
3. Accepts input with probability $\frac{p_1p_2}{p_1+p_2+p_1p_2}$.

1. $w \in L_1$ and $w \in L_2 \longrightarrow$ input is accepted with probability

$$\frac{p_2}{p_1+p_2+p_1p_2} \cdot p_1 + \frac{p_1}{p_1+p_2+p_1p_2} \cdot p_2 + \frac{p_1p_2}{p_1+p_2+p_1p_2} \cdot 1 = \frac{3p_1p_2}{p_1+p_2+p_1p_2}$$

2. $w \in L_1$ and $w \notin L_2 \longrightarrow$ input is accepted with probability at least

$$\frac{p_2}{p_1+p_2+p_1p_2} \cdot p_1 + \frac{p_1p_2}{p_1+p_2+p_1p_2} \cdot 1 = \frac{2p_1p_2}{p_1+p_2+p_1p_2}$$

3. $w \notin L_1$ and $w \in L_2 \longrightarrow$ input is accepted with probability at least

$$\frac{p_1}{p_1+p_2+p_1p_2} \cdot p_2 + \frac{p_1p_2}{p_1+p_2+p_1p_2} \cdot 1 = \frac{2p_1p_2}{p_1+p_2+p_1p_2}$$

4. $w \notin L_1$ and $w \notin L_2 \longrightarrow$ input is rejected with probability at least

$$\frac{p_2}{p_1 + p_2 + p_1 p_2} \cdot p_1 + \frac{p_1}{p_1 + p_2 + p_1 p_2} \cdot p_2 = \frac{2p_1 p_2}{p_1 + p_2 + p_1 p_2}$$

So automaton K recognizes L with the probability at least

$$\frac{2p_1 p_2}{p_1 + p_2 + p_1 p_2} = \frac{1}{2} + \frac{3 - (\frac{1}{p_1} + \frac{1}{p_2})}{4(1 + \frac{1}{p_1} + \frac{1}{p_2})} > \frac{1}{2}$$

□

All this has also a nice geometric interpretation. We are going to build a linear function f from probabilities x_1, x_2 to probability x such that $f(p_1, p_2) \geq \frac{1}{2} + \varepsilon$, $f(p_1, 0) \geq \frac{1}{2} + \varepsilon$, $f(0, p_2) \geq \frac{1}{2} + \varepsilon$, $f(1 - p_1, 1 - p_2) \leq \frac{1}{2} - \varepsilon$. Geometrically we consider a plane x, y where each word w is located in a point (x, y) , where x is probability that K_1 accepts w and y is the probability, that K_2 accepts w .

S_1 is the place where lies all words that do not belong to L . S_2 is the place where lies all words that belong to L .

If we can (Fig.12) separate these two parts with a line $ax + by = c$ then we can construct automaton " $K = aK_1 + bK_2$ " with c as isolated cut point. If we can not (Fig.13) then this method doesn't help. And as it was shown higher sometimes none of other methods can help, too.

Case when $p_1 = p_2 = \frac{2}{3}$ (Fig.14) is the limit case. If any of probabilities were a little bit greater then this method would help.

Sometimes it may be that there are no words w such that K_1 or K_2 would reject with probability $1 - t$ or greater. Then (Fig.15) you can see that now it is easier to make such a line so the condition $\frac{1}{p_1} + \frac{1}{p_2} < 3$ can be weakened (the probabilities in Fig.15 are the same as in Fig.13). In the limit case when rejecting probabilities are only p_1 and p_2 , S_1 is the point $(1 - p_1, 1 - p_2)$ (Fig.16). So with any p_1 and p_2 you can separate S_1 from S_2 with a line, from what it follows you can always construct $K = K_1 \cup K_2$.

Now it is clear that the languages L_2 and L_3 defined in section 3 cannot be recognized with probability greater than $\frac{2}{3}$ so the construction presented there is best possible.

Corollary 3.3. *If 2 languages L_1 and L_2 are recognizable by a QFA with probabilities p_1 and p_2 and $p_1 > 2/3$ and $p_2 > 2/3$, then $L = L_1 \cup L_2$ is recognizable by QFA with probability $p_3 > 1/2$.*

Proof. Follows immediately from Theorem 3.3. □

4 More "forbidden" constructions

If we allow the "two cycles in a row" construction, Theorem 2.2 is not longer true. More and more complicated "forbidden fragments" that imply non-recognizability by a QFA are possible.

Theorem 4.1. *Let L be a language and M be its minimal automaton. If M contains a fragment of the form shown in Figure 10 where $a, b, c, d, e, f, g, h, i \in \Sigma^*$ are words and $q_0, q_a, q_b, q_c, q_{ad}, q_{ae}, q_{bd}, q_{bf}, q_{ce}, q_{cf}$ are states of M and*

1. *If M reads $x \in \{a, b, c\}$ in the state q_0 , its state changes to q_x .*
2. *If M reads $x \in \{a, b, c\}$ in the state q_x , its state again becomes q_x .*
3. *If M reads any string consisting of a, b and c in a state q_x ($x \in \{a, b, c\}$), it moves to a state from which it can return to the same state q_x by reading some (possibly, different) string consisting of a, b and c .*
4. *If M reads $y \in \{d, e, f\}$ in the state q_x ($x \in \{a, b, c\}$), it moves to the state q_{xy} .²*

² Note: we do not have this constraint (and the next two constraints) for pairs $x = a, y = f$, $x = b, y = e$ and $x = c, y = d$ for which the state q_{xy} is not defined.

5. If M reads $y \in \{a, b, c\}$ in a state q_{xy} , its state again becomes q_{xy} .
6. If M reads any string consisting of d, e and f in the state q_{xy} it moves to a state from which it can return to the same state q_{xy} by reading some (possibly, different) string consisting of d, e and f .
7. Reading g in the state q_{ad} , h in the state q_{bf} and i in the state q_{ce} leads to accepting states. Reading h in the state q_{ae} , i in the state q_{bd} , g in the state q_{cf} leads to rejecting states.

then L is not recognizable by a QFA.

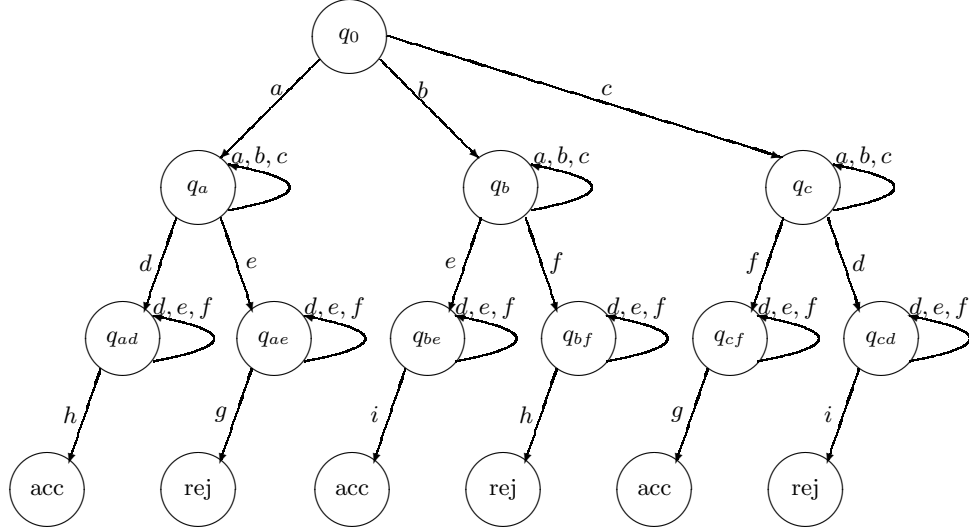


Fig. 10. Conditions of theorem 4.1

Proof. For a contradiction, assume that Q is a QFA that recognizes L with a probability $1/2 + \epsilon$. We construct 6 words such that Q gives a wrong answer on at least one of them.

Let ψ be a superposition of QFA corresponding to the state q_0 (the superposition after reading some word w that leads to q_0). Similarly to the proof of Theorem 2.1, we consider decompositions $E_{non} = E_1^x \oplus E_2^x$ for all $x \in \{a, b, c\}^*$ and take $E_1 = \cap_x E_1^x$, $E_2 = E_{non} - E_1$.

Let $\psi = \psi_1 + \psi_2$, $\psi_1 \in E_1$, $\psi_2 \in E_2$. Similarly to the proof of Theorem 2.1, there is a word $a' \in \{a, b, c\}$ with the first letter a such that $\|V_{a'}'(\psi_1) - \psi_1\| \leq \delta$ and $\|V_{a'}'(\psi_2)\| \leq \delta$ where $\delta = \epsilon/20$. Also, there are words b' and c' with the first letters b and c and the same property.

Next, we consider the decompositions $E_{non} = E_1^x \oplus E_2^x$ for all $x \in \{d, e, f\}^*$ and take $E_3 = \cap_x E_3^x$, $E_4 = E_{non} - E_3$. Let $\psi_1 = \psi_3 + \psi_4$, $\psi_3 \in E_3$, $\psi_4 \in E_4$. Let $d', e', f' \in \{d, e, f\}^*$ be words with the first letters d, e and f such that $\|V_{d'}'(\psi_3) - \psi_3\| \leq \delta$ and $\|V_{d'}'(\psi_4)\| \leq \delta$ (and similar inequalities hold for e' and f').

Let p_0 be the probability of accepting while reading the left endmarker κ and the word w that leads to the superposition ψ_0 . Let p_a, p_b, p_c be the probabilities of accepting while reading a', b' and c' if the starting superposition is ψ . Let p_d, p_e and p_f be the probabilities of accepting while reading a', b' and c' if the starting superposition is ψ_1 . Let p_g, p_h and p_i be the probabilities of accepting while reading $g\$$, $h\$$ and $i\$$ if the starting superposition is ψ_3 .

Lemma 4.1. Let $p_{a'd'g}$ be the probability of accepting the word $wa'd'g$. Then,

$$|p_{a'd'g} - (p_0 + p_a + p_d + p_g)| \leq 12\delta.$$

Proof. $p_{a'd'g}$ is the sum of probabilities of accepting while reading κw , accepting while reading a' , accepting while reading d' and accepting while reading g . The first two probabilities are exactly p_0 and p_a .

The probability of accepting while reading d' may differ from p_d because the state of Q after reading $\kappa wa'$ is $V'_{a'}(\psi)$ and the state used to define p_d is ψ_1 . However, these two probabilities differ by at most 4δ because

$$\|V'_{a'}(\psi) - \psi_1\| \leq \|V'_{a'}(\psi_1) - \psi_1\| + \|V'_{a'}(\psi_2)\| \leq 2\delta$$

and the probability distributions resulting from observing $V'_{a'}(\psi)$ and ψ_1 can differ by at most twice the distance between superpositions (Lemma 2.1).

Similarly, the distance between the state of Q after reading $\kappa a'd'$ and ψ_3 is at most 4δ and this implies that the probability of accepting while reading g portion of $\kappa wa'd'g$ differs from p_g by at most 8δ . Therefore, the difference between $p_{a'd'g}$ and $(p_0 + p_a + p_d + p_g)$ is at most $4\delta + 8\delta = 12\delta$.

Similar bounds are true for probabilities of accepting $wb'f'h$, $wc'e'i$, $wa'e'h$, $wb'd'i$, $wc'f'g$. (We denote these probabilities $p_{b'f'h}$, $p_{c'e'i}$, $p_{a'e'h}$, $p_{b'd'i}$, $p_{c'f'g}$.) By putting the bounds for $p_{a'd'g}$, $p_{b'f'h}$, $p_{c'e'i}$ together, we get

$$|(p_{a'd'g} + p_{b'f'h} + p_{c'e'i}) - (3p_0 + p_a + p_b + p_c + p_d + p_e + p_f + p_g + p_h + p_i)| \leq$$

$$|p_{a'd'g} - (p_0 + p_a + p_d + p_g)| + |p_{b'f'h} - (p_0 + p_b + p_f + p_h)| + |p_{c'e'i} - (p_0 + p_c + p_e + p_i)| \leq 36\delta.$$

Putting the bounds for $p_{a'e'h}$, $p_{b'd'i}$, $p_{c'f'g}$ together gives

$$|(p_{a'e'h} + p_{b'd'i} + p_{c'f'g}) - (3p_0 + p_a + p_b + p_c + p_d + p_e + p_f + p_g + p_h + p_i)| \leq 36\delta,$$

$$|(p_{a'd'g} + p_{b'f'h} + p_{c'e'i}) - (p_{a'e'h} + p_{b'd'i} + p_{c'f'g})| \leq 72\delta.$$

However, each of $p_{a'd'g}$, $p_{b'f'h}$, $p_{c'e'i}$ is the probability of accepting a word in L and must be at least $1/2 + \epsilon$ and each of $p_{a'e'h}$, $p_{b'd'i}$, $p_{c'f'g}$ is the probability of accepting a word not in L and must be at most $1/2 - \epsilon$. Therefore,

$$(p_{a'd'g} + p_{b'f'h} + p_{c'e'i}) - (p_{a'e'h} + p_{b'd'i} + p_{c'f'g}) \geq 6\epsilon = 120\delta.$$

A contradiction. □

The existence of the “forbidden construction” of Theorem 4.1 does not imply the existence of any of previously shown “forbidden constructions”.

This can be shown as follows. Consider the alphabet $\Sigma = \{a, b, c, d, e, f, g, h, i\}$ and languages of the form $L_{x,y,z} = x(a|b|c)^*y(d|e|f)^*z$ where $x \in \{a, b, c\}$, $y \in \{d, e, f\}$, $z \in \{g, h, i\}$. Our language L will be the union of languages $L_{x,y,z}$ corresponding to black squares in Figure 11.

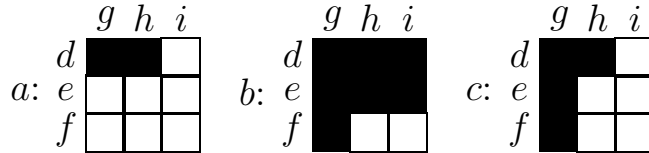


Fig. 11. The language L

Theorem 4.2. *The minimal automaton of L does not contain the “forbidden construction” of Theorem 2.1.*

Proof. The minimal automaton of L has a structure similar to Figure 10, with some more states. Similarly to Figure 10, the states of the minimal automaton of L can be partitioned into 4 levels:

1. The starting state (nothing read so far).
2. The states after reading a, b or c .
3. The states after reading a, b or c and d, e or f .
4. The states after reading a, b or c, d, e or f and g, h or i .

If we look for the “forbidden construction” of Theorem 2.1, then q_2 and q_3 should be in the 2nd or 3rd level. (q_2 or q_3 cannot be in the 1st level because, after reading any letter in the starting state, M leaves it and never returns. Also, q_2 or q_3 cannot be in the 4th level because every state in it is “all-accepting” or “all-rejecting”.) This leaves us with 3 possible cases.

1. q_2 and q_3 are both states on the 2nd level (after the automaton has read a, b or c).
The sets of words that are accepted from q_2 and q_3 correspond to black pieces in 3×3 squares in Figure 11. For any two of these three squares, the black pieces in one of them are subset of the black pieces in the other. (And this means there is no words z_1, z_2 such that z_1 gets accepted from q_2 but not from q_3 and z_2 gets accepted from q_3 and not from q_2 .)
2. q_2 and q_3 are two of the 9 states on the 3rd level (after reading one of a, b or c and one of d, e or f).
The sets of words that lead to acceptance correspond to rows in Figure 11. One can easily see that any two of them are subsets of one another.
3. One of q_2 and q_3 is on the 2nd level and the other is on the 3rd level.
W. l. o. g., assume that q_2 is on the 2nd level and q_3 is on the 3rd level. Then, the word y that leads the automaton M from q_1 to q_3 must contain one of letters d, e and f . However, reading d, e or f in the state q_2 would lead M to a state in the 3rd level from which it cannot return to q_2 (and, therefore, the condition 6 of Theorem 2.1 is violated).

In all 3 cases, we see that one of conditions of Theorem 2.1 is violated. Therefore, the minimal automaton M does not contain the “forbidden construction” of Theorem 2.1. \square

However, one can easily see that the minimal automaton of L contains the “forbidden construction” of Theorem 4.1. (Just take q_0 to be the starting state and make a, b, \dots, i of Theorem 4.1 equal to corresponding letters in the alphabet Σ .) This means that the existence of “forbidden construction” of Theorem 4.1 does not imply the existence of the “forbidden construction” of Theorem 2.1.

Theorem 4.1 can be generalized to any number of levels (cycles following one another) and any number of branchings at one level as long as every arc from one vertex to other is traversed the same number of times in paths leading to accepting states and in paths leading to rejecting states.

A general “forbidden construction” is as follows.

Level 1 of such a construction consists of a state q_1 and some words a_{11}, a_{12}, \dots

Level 2 consists of the states q_{21}, q_{22}, \dots where the automaton goes if it reads one of words of Level 1 in a state in Level 1. We require that, if the automaton starts in one of states of Level 2 and reads any string consisting of words of Level 1 it can return to the same state reading some string consisting of these words. Level 2 also has some words a_{21}, a_{22}, \dots

Level 3 consists of the states q_{31}, q_{32}, \dots where the automaton goes if it reads one of words of Level 2 in a state in Level 2. We require that, if the automaton starts in one of states of Level 3 and reads any string consisting of words of Level 2 it can return to the same state reading some string consisting of these words. Again, Level 3 also has some words a_{31}, a_{32}, \dots

Level n consists of the states q_{n1}, q_{n2}, \dots where the automaton goes if it reads one of words of Level $n - 1$ in a state in Level $n - 1$.

Let us denote all different words in this construction as $a_1, a_2, a_3, \dots, a_m$.

For a word a_i and a level j we construct sets of states B_{ij} and D_{ij} . A state q in level $j + 1$ belongs to B_{ij} if the word a_i belongs to level j and M moves to q after reading a_i in some state in level j . A state belongs to D_{ij} if this state belongs to the Level n and it is reachable from B_{ij} .

Theorem 4.3. *Assume that the minimal automaton M of a language L contains the “forbidden construction” of the general form described above and, in this construction, for each D_{ij} the number of accepting states is equal to the number of rejecting states. Then, L cannot be recognized by a 1-way QFA.*

Theorems 2.1 and 4.1 are special cases of this theorem (with 3 and 4 levels, respectively).

References

- ABFK 99. Andris Ambainis, Richard Bonner, Rūsiņš Freivalds, Arnolds Ķikusts. Probabilities to accept languages by quantum finite automata. *Proc. COCOON'99*. Also quant-ph/9904066³.
- AF 98. Andris Ambainis and Rūsiņš Freivalds. 1-way quantum finite automata: strengths, weaknesses and generalizations. *Proc. FOCS'98*, p. 332–341. Also quant-ph/9802062.
- ANTV 98. Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, Umesh Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. *Proc. STOC'99*. Also quant-ph/9804043.
- BV 97. Ethan Bernstein, Umesh Vazirani, Quantum complexity theory. *SIAM Journal on Computing*, 26:1411–1473, 1997.
- BP 99. Alex Brodsky, Nicholas Pippenger. Characterizations of 1-way quantum finite automata. quant-ph/9903014.
- G 00. Jozef Gruska. Descriptive complexity issues in quantum computing. *Journal of Automata, Languages and Combinatorics*, 5:191–218, 2000.
- KS 76. John Kemeny, J. Laurie Snell. *Finite Markov Chains*. Springer-Verlag, 1976.
- K 98. Arnolds Ķikusts. A small 1-way quantum finite automaton. quant-ph/9810065.
- KW 97. Attila Kondacs and John Watrous. On the power of quantum finite state automata. In *Proc. FOCS'97*, p. 66–75.
- MT 69. A. Meyer, C. Thompson. Remarks on algebraic decomposition of automata. *Mathematical Systems Theory*, 3:110–118, 1969.
- MC 97. C. Moore, J. Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237:275–306, 2000. Also quant-ph/9707031.
- N 99. Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. *Proc. FOCS'99*. Also quant-ph/9904093.

³ quant-ph preprints are available at <http://www.arxiv.org/abs/quant-ph/preprint-number>

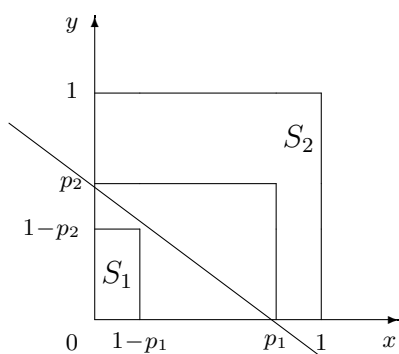


Fig. 12.

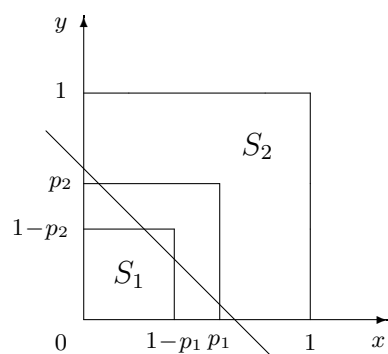


Fig. 13.

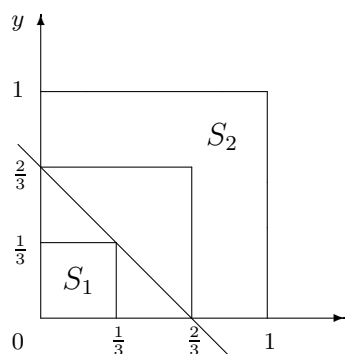


Fig. 14.

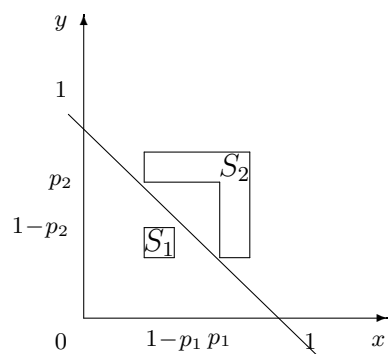


Fig. 15.

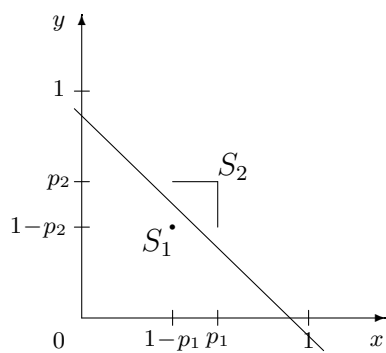


Fig. 16.